<u>REMARKS</u>

Claims 1 and 3-13 are pending in this application. All of the pending claims are rejected. Reconsideration and further examination are requested.

The presently claimed invention helps to provide secure communications in a network. VPNs and IPsec tunneling use point-to-point connections between sites. This creates a scalability problem because the amount of data stored to support N connections in the network grows at the rate of N^2-1. In a network having a thousand endpoints, data may need to be stored identifying paths and authentication for the million connections between the endpoints. Various proposals have been made to overcome the scalability issues associated with VPNs, but all have drawbacks. For example, at least one proposed solution requires that a high level of trust be placed on the Service Provider to protect the Customer data. Encrypted tunneling can be used to lower the need for such trust. However, overlaying traditional encrypted tunneling methods on top of the IP VPN structure simply introduces more point-to-point security associations, thereby eliminating the scalability benefits of the IP VPN architecture. The presently claimed invention helps to overcome these drawbacks by utilizing a group security association instead of multiple point-to-point security associations, i.e., the same group security association for different connections.

As discussed in the Background, point-to-point and group security associations are both well known. However, application of the same group security association to non-group point-to-point communications is not only different, but also counter-intuitive. Prior to this invention, group security was applied to a group of devices that shared the same connection, e.g., multicast. Since the devices share the same connection, there is no concern about different members of the group sharing the same security association. However, this lack of concern does not hold true

for members of a group that do not share the same connection, i.e., members exchanging different (non-group) communications. Consequently, each non-group connection has traditionally been assigned a unique point-to-point security association. The presently claimed invention is distinct because it utilizes a group security association instead of multiple point-to-point security associations, i.e., the same group security association for different connections. This solution is counter-intuitive because members not sharing a connection could technically obtain access to each other's data. However, the possibility of such an occurrence is reduced by applying the group security association at trusted edge devices.

Claims 1, 3, 7 and 9-13 are rejected under 35 U.S.C. 103(a) based on US 2004/0044891 (Hanzlik) in view of US 6,891,793 (Suzuki). As currently amended the claims clearly distinguish the cited combination. Hanzlik teaches use of a security association for communications between members of a group, but fails to teach utilizing a group security association instead of multiple point-to-point security associations, i.e., the same group security association for *different connections*. Again, group security associations are well known, but the same group security association has never been used for different connections between different sets of devices because that is the purpose of point-to-point security associations. The Office cites Suzuki as disclosing the recited border router. Border routers are generally known, but not those which distribute and use the same group security association for different connections between different sets of devices. Claims 1, 3, 7 and 9-13 therefore distinguish the cited combination.

Claims 4-6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanzlik and Suzuki in view of US 2004/0006708 (Mukherjee). Claims 4-6 and 8 are allowable for the same reasons stated above. If an independent claim is nonobvious under 35 U.S.C. 103, then any

claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Claims 7-9 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. In particular, the examiner asserts that "a network device" could be interpreted to be either a machine or software. Claims 7-9 are currently amended to recite an apparatus. The Office will kindly note that implementation in software versus hardware is merely a design decision, and there is no prohibition against protecting both implementations. Applicant hopes that the current language is sufficient to satisfy the panel that reviews section 101 matters.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited. Should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

September 22, 2008
Date

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37,272
Attorney/Agent for Applicant(s)
Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton, MA 01720
(978) 264-4001

Docket No. 120-279
Dd: 08/23/2008